IN THE SPECIFICATION (MARKED-UP VERSION):

Paragraph beginning on page 1, line 16.

This is a continuation-in-part of a non-provisional patent application Serial No. 09/457,463 filed December 9, 1999 now [_____], for "Multi-Tier Digital TV Programming for Content Distribution", which is commonly assigned herewith to International Business Machines. The above aforementioned patent application is incorporated hereinto in its entirety by reference.

Paragraph beginning on page 160, line 4

The process flow 2100 begins in step 2102, a "Buy" and "Catalog" icons are displayed. User input, step 2104 is received. A test is made to determine the user selection, steps 2106 and 2108, of "Buy or Catalog" during the broadcast of a program 2204. If "Buy" is selected, the user is asked to identify themselves for billing purposes, step 2110. The embodiment shown in steps 2110-2116 and FIG. 24. uses a "smart card" and an associated personal identification number (PIN). Other billing mechanisms are possible, including the use of a debit card. Once the user identifies himself or herself, the download begins, step 2118. If "Catalog" is selected in step 2106, a menu panel of purchasable products is displayed, step 2120, and the user may navigate among them via a selection cursor (steps not shown). User input is received in step 2122. If this input it "Buy" the viewer proceeds through the authentication process, 2110-2116. If the input is "Exit", the viewer returns to the "Buy" and "Catalog" choices, step 2126. Upon successful authentication, the download process begins with an optional message indicating this to the viewer, as shown in FIG. 26. Note that all graphic images are overlaid on top of video that is not interrupted by the consumer's[(?)] purchasing activity.

MARKED-UP COPY

1. (Once Amended) A method of securely providing data to a user's system over a web broadcast infrastructure with a plurality of channels, the method comprising the steps of:

encrypting the data using a first encrypting key, wherein the first encrypting key is self-contained with all the information necessary to decrypt the data encrypted with the first encrypting key;

encrypting the first decrypting key, using a second encrypting key;

broadcasting promotional metadata related to at least part of the encrypted data on a first web broadcast channel [fro] for reception by at least one user's system;

broadcasting at least part of the encrypted data over a second broadcast channel; and

transferring the encrypted first decrypting key, which has been encrypted with the second encrypting key, to the user's system via a computer readable medium.

5. (Once Amended) The method as defined in claim 1, wherein the step of broadcasting at least part of the encrypted data over a second web broadcast channel includes broadcasting the encrypted data in a format compatible with [DirecPC™] satellite broadband Internet service.

7. (Once Amended) A method of securely receiving data on a user's system from a web broadcast infrastructure with a plurality of channels, the method comprising the steps of:

receiving promotional metadata from a first web broadcast channel, the promotional metadata related to data available for reception;

assembling at least part of the promotional metadata into a promotional offering for review by a user;

selecting by a user, data to be received related to the promotional metadata;

receiving data from a second web broadcast channel, the data selected from the promotional metadata, and wherein the data has been previously encrypted using a first encrypting key, wherein the first encrypting key is self-contained with all the information necessary to decrypt the data encrypted with the first encrypting key; and

receiving the first decrypting key via a computer readable medium, the first decrypting key for decrypting at least some of the data received via the second web broadcast channel.

12. The method as defined in claim 7, wherein the step of receiving data from a second web broadcast channel includes receiving data in a format compatible with [DirecPC™] satellite broadband Internet service.

19. (Once Amended) A system for securely providing data to a user's system over a web broadcast infrastructure with a plurality of channels, the system comprising:

a content system;

a first public key;

a first private key, which corresponds to the first public key;

a data encrypting key, ;

a data decrypting key for decrypting data encrypted using the data encrypting key , wherein the data decrypting key is self-contained with all the information necessary to decrypt the data encrypted with the data decrypting key;

first data encryption means for encrypting data so as to be decryptable only by the data decrypting key;

second data encryption means, using the first public key, for encrypting the data decrypting key;

a clearing house;

a broadcast center, for broadcasting to one or more user's systems on a first web broadcast channel, promotional metadata related to data being broadcasted on a second web broadcast channel, and broadcasting on the second broadcast channel data encrypted with the data encrypting key;

first transferring means for transferring the data decrypting key which has been encrypted to the clearing house, wherein the clearinghouse possesses the first private key;

first decrypting means for decrypting the data decrypting key using the first private key;

a second public key;

a second private key; which corresponds to the second public key;

re-encryption means for re-encrypting the data decrypting key using the second public key;

second transferring means for transferring the re-encrypted data decrypting key to the user's system, wherein the user's system possesses the second private key; and

second decrypting means for decrypting the re-encrypted data decrypting key using the second private key.

21. (Once Amended) A user's system for securely receiving data from a web broadcast infrastructure with a plurality of channels, comprising:

a receiver for receiving promotional metadata from a first web broadcast channel, the promotional metadata related to data available for reception;

an interface to an output device for presenting at least part of the promotional metadata for review by a user;

an interface to an input device for receiving a selection by a user of the data to be received related to the promotional metadata;

a controller for controlling the receiver to receive data from a second web broadcast channel, the data selected from the promotional metadata, and wherein the data has been previously encrypted using a first encrypting key, wherein the first encrypting key is self-contained with all the information necessary to decrypt the data encrypted with the first encrypting key; and

an interface for receiving the first decrypting key via a computer readable medium, the first decrypting key for decrypting at least some of the data received via the second web broadcast channel.

24. The user's system as defined in claim 21, wherein the receiver is adapted to receive data broadcasted in a format compatible with [DirecPC™] satellite broadband Internet service.

REMARKS

Applicants have studied the Office Action dated May 16, 2002 and have made amendments to the claims. It is submitted that the application, as amended, is in condition for allowance. By virtue of this amendment, claims 1-25 are currently pending in the present application. Reconsideration and allowance of the pending claims in view of the above amendments and the following remarks are respectfully requested. In the Office Action, the Examiner:

- objected to the specification for various informalities;
- objected to FIG. 27 because of missing numbers;
- objected to claims 5, 12, and 24 because of the use of the trademark/tradename DirecPC;
- objected to claim 1 because of the misspellings of "for" and "one";
- rejected claims 1-3, 5, 7-16, and 21-25 under 35 U.S.C. § 103 as being unpatentable over (U.S. 6,337,911) in view of Dillon (U.S. 6,351,467); and
- rejected claims 4 and 6 under 35 U.S.C. § 103 as being unpatentable over Dillon (U.S. 6,337,911) in view of Dillon (U.S. 6,351,467), and further in view of Cablevision(periodical).

The Applicants acknowledge that informal drawings have been filed and are acceptable for examinations purposes only. Upon allowance, the Applicants will submit the required formal drawings. FIG. 27 has been corrected to include numbers 2702 and 2704 as described and referenced in the original application

The abstract has been amended to be a single paragraph, no new matter has been added.

Claim 1 has been amended to correct the misspellings of "for" and "one."

Rejection Under 35 U.S.C. §112 ¶2

As noted above, the Examiner rejected claims 5, 12, and 24 under 35 U.S.C. § 112 ¶2 for containing the trademark/tradename DirecPC™. The claims have been amended to recited a type of broadcasting in more specifically "satellite broadband Internet service." Support for this language

is found in the specification as originally filed at least on page 17, lines 13, page 20, line 18, page 118, line 15. The Applicants respectfully submit that the Examiner's rejection under 35 U.S.C. § 112 has been overcome and the Examiner's rejection should be withdrawn.

Rejection Under 35 U.S.C. §103(a)

As noted above, the Examiner rejected claims 1-3, 5, 7-16, and 21-25 under 35 U.S.C. § 103 as being unpatentable over Dillon (U.S. 6,337,911) in view of Dillon (U.S. 6,351,467). Independent claims 1, 7, 19, and 212 have been amended to distinguish over the "key seed ID" identifying the key seed needed to decrypt the document" in Dillon '911 taken alone or in view of Dillon '467. The Dillon '911 reference teaches that the "key seed ID" is sent as opposed to a decrypting key as recited in the present invention. In the words of Dillon at col. 6, lines 57-58:

> "After broadcast center 150 sends the announcement message for a document, it prepares to send the document itself. The document is packetized, encrypted, and broadcast over communications link 140. As broadcast receiver 120 receives each encrypted packet, it determines whether it is a packet for which broadcast receiver 120 has a key." (Emphasis Added).

And as the Examiner points out in Dillon at col. 6, lines 44-48:

> "The announcement message is received and decrypted by broadcast receiver 120 and passed to file broadcast receiver 112. If the announced document is on the list of documents of interest, file broadcast receiver 112 sends a load request including the key seed ID to security engine 130." (Emphasis Added).

Accordingly, Dillon '911 teaches taking the "key seed ID" and encrypting it. The "key seed ID" as taught by Dillon is used to generate the decrypting key in security engine 130. See col. 4, lines 59-67 continuing onto col. 5, lines 1-6. In the words of Dillon at col. 8, lines 33-44:

> "In executing function F3, broadcast center 150 periodically, e.g., monthly, sends account status information to each of the plurality of receiving computers, including receiving computer 110. The account information is tailored to the receiving computer and includes a statement of its receiver's status (e.g., satisfactory, overdrawn, limited access, etc.). The account information also includes core information required by security engine 130 to create keys to decrypt electronic

documents. Although the account information is broadcast in the clear, the contents of the account information is encrypted in such a way that only security engine 130 may access and decrypt the account information." (Emphasis Added).

In contrast, the independent claims 1, 7, 19, and 21 of the present invention have been amended to describe the first encrypting key as "self-contained with all the information necessary to decrypt the data encrypted with the first encrypting key." Support for this language is found in the present invention as originally filed in FIG. 6 items 623 and in the specification at least pages 43 - 150. This is very important since the self-contained key itself and not a "key seed ID" as taught by either of the Dillon references. This self-contained key is sent to the End User System but only after the "first decrypting key is encrypted," using a second encrypting key." The Dillon references nowhere teaches or suggests such levels of security. In contrast Dillon is relying on pre-sending key information to the security engine 130 on a periodic basis so that the security engine 130 is able "to create keys to decrypt electronic documents." The present invention eliminates this step of pre-sending account status information on a periodical basis because in the present invention, the first encrypting key is "self-contained with all the information necessary to decrypt the data encrypted with the first encrypting key." Accordingly, the present invention distinguishes over Dillon '911 taken alone or in view of Dillon '467 for at least this reason.

Continuing further, the present invention relies on the a second encrypting key which is a public key of a trusted third party i.e. Clearing house(s) 105. Dillon '911 taken alone or in view of Dillon '467 does not show this level of security control using public keys of trusted third parties rather Dillon is using a "key seed ID" which is sent to decrypt the document which has been decrypted. See at least Dillon '911 at col. 6, lines 57-58 and col. 6, lines 44-48. By using public key infrastructure, the present invention is not limited to pre-sending "key seed Ids" to generate local decryption keys at the security engine 130. The public key infrastructure allows any type of self-contained key to be used including keys of different lengths and therefore different encryption strengths. In the present invention each piece of content or data can be dynamically encrypted with a different type of key strength without the requirement to pre-send the decrypting key to an end user system as taught by Dillon '911. Accordingly, the present invention distinguishes over Dillon '911 taken alone or in

view of Dillon '467 for at least this reason as well.

In the Office Action at page 3, the Examiner correctly states "*Although Dillon '991 does not specifically disclose the details of broadcasting using multiple channels*" however, the Examiner goes onto combine Dillon '467.[1] The Examiner states Dillon '467 "*teaches a system and method for multicasting multimedia content such that Applicants' step of broadcasting at least part of the encrypted data...*" The Applicants respectfully disagree. The present invention recites broadcasting at least part of the encrypted data but where the data was encrypted with a first encrypting key, where wherein the first encrypting key is self-contained with all the information necessary to decrypt the data encrypted with the first encrypting key. The "key seed" as disclosed in Dillon requires information to be present to the security engine 130. Accordingly, the present invention distinguishes over this step in Dillon '467 as well.

The Examiner recites 35 U.S.C. §103. The Statute expressly requires that obviousness or non-obviousness be determined for the claimed subject matter "as a whole," and the key to proper determination of the differences between the prior art and the present invention is giving full recognition to the invention "as a whole." The Dillon '911 reference, taken alone or in view of Dillon '467, simply does not suggest, teach or disclose the patentably distinct limitation of:

- Claims 1, 7, 21

  wherein the first encrypting key is self-contained with all the information necessary to decrypt the data encrypted with the first encrypting key

- Claim 19

  wherein the data decrypting key is self-contained with all the information necessary to decrypt the data encrypted with the data decrypting key;

The limitations taken "as a whole" in independent claims 1, 7, 19, and 21 are not present in Dillon '911 reference taken alone or in view of Dillon '467.

---

[1] Applicants make no statement whether such combination is even proper.

Moreover, the Federal Circuit has consistently held that when a §103 rejection is based upon a modification of a reference that destroys the intent, purpose or function of the invention disclosed in the reference, such a proposed modification is not proper and the *prima facie* case of obviousness can not be properly made. See In re Gordon, 733 F.2d 900, 221 USPQ 1125 (Fed. Cir. 1984). Here the intent, purpose and function of the present invention to use "self-contained" decrypting key is destroyed by the use of "key seed Ids" as taught in Dillon 911 taken alone or in view of Dillon '467. Not only does the present invention eliminate the need to "to create keys to decrypt electronic documents" in security engine 130 as required by Dillon, but the present invention makes use of the many advantages of a public key infra structure. This combination, as suggested by the Examiner, destroys the intent and purpose of the present invention of "self-contained" "decrypting keys." Accordingly, the present invention is distinguishable over Dillon 911 taken alone or in view of Dillon '467 for this reason as well.

Continuing further, when there is no suggestion or teaching in the prior art for a first encrypting key which is self-contained with all the information necessary to decrypt the data encrypted with the first encrypting key, the suggestion cannot come from the Applicant's own specification. The Federal Circuit has repeatedly warned against using the Applicant's disclosure as a blueprint to reconstruct the claimed invention out of isolated teachings of the prior art. See MPEP §2143 and Grain Processing Corp. v. American Maize-Products, 840 F.2d 902, 907, 5 USPQ2d 1788 1792 (Fed. Cir. 1988) and In re Fitch, 972 F.2d 160, 12 USPQ2d 1780, 1783-84 (Fed. Cir. 1992). The prior art reference Dillon '911 taken alone or in view of Dillon '401 does not suggest, teach, or mention the use of "self-contained" encrypting keys.[2]

---

[2] Very recently, the Federal Circuit again took up the identical question of Obviousness in combining references in the case In re Sang Su Lee, No. 00-1158 (January 18, 2002). In this case Board of Patent Appeals rejected all of Applicant's pending claims as obvious under § 103. The Federal Circuit vacated and remanded. Citing two prior art references, the Board stated that a person of ordinary skill in the art would have been motivated to combine the references based on "common knowledge" and "common sense," but it did not present any specific source or evidence in the art that would have otherwise suggested the combination. The Federal Circuit held that the Board's rejection of a need for any specific hint or suggestion in the art to combine the references was both legal error and arbitrary agency action subject to being set aside by the

For the foregoing reasons, independent claims 1, 7, 19 and 21 as amended distinguish over Dillon '911 in view of Dillon '467. Claims 2-3, 5, 8-16, and 22-25 depend from claims 1, 7, and 21 respectively, since dependent claims contain all the limitations of the independent claims, claims 2-3, 5, 8-16, and 22-25 distinguish over Dillon '911 taken alone or in view of Dillon '401, as well, and the Examiner's rejection should be withdrawn.

Rejection Under 35 U.S.C. §103(a)

As noted above, the Examiner rejected claims 4 and 6 under 35 U.S.C. § 103 as being unpatentable over Dillon (U.S. 6,337,911) in view of Dillon (U.S. 6,351,467), and further in view of Cablevision(periodical). Independent claim 1 has been amended to distinguish over Dillon (U.S. 6,337,911) in view of Dillon (U.S. 6,351,467) as described above. The Examiner goes on to combine Cablevision(periodical).[3] The Cablevision reference nowhere suggests or teaches "wherein the first encrypting key is self-contained with all the information necessary to decrypt the data encrypted with the first encrypting key." Accordingly, claim 1 of the present invention distinguishes over Dillon '911 in view of Dillon '467, and further in view of Cablevision(periodical). Claims 4 and 6 depend from claim 1, since dependent claims contain all the limitations of the independent claims, claims 4 and 6 distinguish over Dillon '911 taken alone or in view of Dillon '401, and further in view of Cablevision(periodical) as well, and the Examiner's rejection should be withdrawn.

Applicants have examined the reference cited by the Examiner as pertinent but not relied upon. It is believed that this reference neither discloses nor makes obvious the invention recited in the present claims. In view of the foregoing, it is respectfully submitted that the application and the claims are

---

court under the Administrative Procedure Act (APA). Accordingly, with the suggestion or motivation found in Johnson, the Examiner has failed to properly establish a *prima facie* case of obviousness of the invention as a "whole." The Applicants submit the present invention distinguishes over Dillon 911 taken alone or in view of Dillon '467 for at least this reason as well.

[3] Applicants make no statement whether such combination is even proper.

in condition for allowance. Further examination and reconsideration of the application, as amended, is requested.

CONCLUSION

In view of the foregoing, Applicants respectfully submit that all of the grounds for rejection stated in the Examiner's office action have been overcome, and that all claims in the application are allowable. No new matter has been added. It is believed that the application is now in condition for allowance, which allowance is respectfully requested.

PLEASE CALL the undersigned if this would expedite the prosecution of this application.

Respectfully submitted.

August 29, 2002

By: _____

Jon A. Gibbons (Reg. No. 37,333)
Attorney for Applicants
Fleit, Kain, Gibbons, Gutman & Bongini, P.L.
One Boca Commerce Center, Suite 111
551 Northwest 77th Street
Boca Raton, FL 33487
Telephone: (561) 989-9811
Facsimile: (561) 989-9812

PLEASE Direct All Correspondence to Customer Number 23334

150-a99-164amd1.wpd